REMARKS

Reconsideration of the rejections set forth in the Office Action dated 08/25/2004 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-3, 5-15 and 17-22 are pending.

Claims 1-3, 5-15 and 17-22 are rejected.

No claims were amended.

Applicant petitions for a one month extension and has included the petition and corresponding fee authorization herewith.

I. Comments related to the Examiner's Response to Arguments

Applicant has previously amended claims 1, 13, and 20 (in the RCE that was responsive to the office action mailed 05/03/2004) to make them more clear that the server off-loads the computation burden associated with the cryptographic service from the client. These amendments explicitly added a result of the limitations in the claim.

Applicant respectfully believes the Examiner may have confused the difference between a cryptographic service and the cryptographic operations used to encrypt communications between the client and server. The cryptographic service that resides on the server performs cryptographic operations for the client. Thus, the client can off-load, for example, a computationally expensive cryptographic operation to a server that is optimized to perform that cryptographic operation.

To help the Examiner distinguish between a cryptographic service and a cryptographic operation, the applicant offers the following observation that would have been apparent to one skilled in the art on reading the application.

- A cryptographic server provides clients with cryptographic services to perform cryptographic operations by the server instead of by the client.

- These cryptographic operations, in the prior art, would always have been performed by the client.
- Thus, cryptographic operations that are performed by the cryptographic server simply to securely communicate with the client are not encompassed within the meaning of cryptographic service *because those operations would never have been performed by the client.*
- Applicant traverses any argument that asserts or implies that a cryptographic service would encompass a cryptographic operation required to be performed by a server to securely communicate with a client.

In an attempt to advance the prosecution of the instant application, Applicant admits that client-server architectures are well-known in the art; that secure tunnels between two computers over a public network are well known in the art; that cryptographic operations such as modular exponentiation and the use of modular exponentiation to perform public/private Key cryptographic operations are well known in the art; and that cryptographic operations can be used to enable secure communications between computers over a public network. Applicant also admits that no new cryptographic algorithm is disclosed in the instant application.

Applicant respectfully points out to the Examiner that one aspect of the claimed invention is that of using the well-known client-server architecture concept to allow a client (that generally is not optimized to perform cryptographic operations) to request a server (the cryptoserver) to perform cryptographic operations for the client such that the client computer does not need to perform the cryptographic operations to get the results – thus off-loading the burden of performing those cryptographic operations from the client to the cryptoserver. The cryptoserver is optimized to efficiently perform these cryptographic operations (for example, by being placed at a well connected network node and/or by being configured to include specialized cryptographic accelerator hardware (page 16, lines 20-27). Hence, the cryptoserver provides the client with the service of performing cryptographic operations that have been requested by the client for the client. Thus, the cryptoserver off-loads the computational burden of performing the

cryptographic operation from the client. The request for service made by the client to the cryptoserver is made over a secure tunnel between the client and the cryptoserver.

With regard to paragraph 1 of the Office Action dated 08/25/2004: The Examiner has disagreed with the applicant's argument related to McGarvey.

The Examiner references McGarvey Fig. 3 as teaching such a service.

> FIG. 3 illustrates the delegation model of the present invention, which delegates authority from a client 300 to a server machine or process 310. The server machine or process 310 may use this delegated authority to access data or services that are remotely located (i.e. on a different machine in the network) or to access data or services co-located with the server machine or process. Hereinafter, the term "server machine" will be used to refer to the server machine or process receiving the delegated authority. The delegation model depicted in FIG. 3 further comprises a secure communications path 320, a private key system 330 (such as Kerberos), and a protected resource or service 340. The client 300 maintains a client certificate and a private key 305, which it will use for authentication with the server 310 and private key system 330. The connection path 320 is used for sending encrypted messages between the server 310 and the private key system 330. This path may be established using a protocol such as SSL or TLS.
>
> In this delegation model, the client 300 needs services or data from the protected resource or service 340. The client 300 will obtain credentials to enable the server 310 to access the services or data on its behalf. These credentials are obtained by accessing the private key system 330, and they are subsequently delegated to the server machine 310, in a variety of ways that are disclosed below in the preferred embodiments, which are discussed with reference to FIGS. 5-8.
>
> With the delegation model disclosed herein, the client only has access to the private key system through the server machine. This offers a level of protection to the private key system from unauthorized access from the public network.
>
> Four preferred embodiments of the present invention will now be described. Each embodiment provides an independent technique for delegating client authority to a server machine or process. The embodiments are intended to be used independently from one another.

The text related to FIG.3 teaches that a client can delegate its authority to access a protected resource or service by delegating a credential to a server such that the server can access the protected resource or service as an agent of the client. Thus, when McGarvey's client delegates authority to McGarvey's server, McGarvey's server can access the same resources that the client can access. In addition, the McGarvey server and client can communicate using an encrypted data path.

Applicant respectfully, but strongly, traverses the assertion that any reasonable interpretation of a cryptographic service would include McGarvey's authority delegation model.

With regard to paragraph 2 of the Office Action dated 08/25/2004: The Examiner reasserts the interpretation that McGarvey teaches a cryptographic service. Again, applicant must respectfully, but strongly, traverse such an assertion because nothing in McGarvey teaches a cryptographic service, a cryptoserver, or the use of a client-server architecture that functions to off-load cryptographic operations that would be done by the client from the client to the cryptoserver.

With regard to paragraph 3 of the Office Action dated 08/25/2004: The Examiner asserts that McGarvey teaches providing a cryptographic service at the server (citing McGarvey Fig. 6) and arguing that the session key(s) are sent (607) from the private key system to the server to enable the server to decrypt data request coming in from the client and to encrypt the resulting messages to the client (citing column 10, lines 33-36) and thus meeting the limitation of "cryptographic server". Applicant again traverses this argument for the reasons previously presented.

With regard to the unnumbered paragraph after paragraph 3 of the Office Action: Applicant admits that techniques were known at the time of invention for providing a secure tunnel between two computers over the public network. However, applicant does not understand what relevance the — determination of the encryption algorithm used to encrypt a packet — has to the currently pending claims. The provided rational that one of ordinary skill in the art would have been "motivated to receive information at the server from the client utilizing the tunnel as taught in Kirby for determining the type of

encryption algorithm used to encrypt the packet" appears to not address the currently claimed invention. Applicant respectfully requests that the Examiner provide an affidavit fully explaining the Examiner's rational for this assertion.

II. General Comments regarding the claimed invention

The currently claimed invention is directed towards **a cryptographic service**. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22 (as well as the application as a whole).

To summarize, a cryptographic service provider operates a server. The server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the server that provides the service of performing the cryptographic operation. One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a server that performs the requested cryptographic service for the client.

The server thus provides a cryptographic service to a client computer such that the client computer can off-load the computational burden due to cryptographic operations from the client computer to the cryptographic server. The cryptographic operations performed by the server are those that could have been performed by the client.

The invention of previously presented claim 1 is directed to a networked server that provides a cryptographic service. The method includes the following steps.

(a) identifying a client utilizing the network;

(b) establishing a first key;

(c) generating a tunnel on the network;

(d) receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) performing the cryptographic service at the server for the client whereby the server off-loads a computational burden associated with the cryptographic service from the client.

Thus, the claimed invention is directed to providing a cryptographic service from a networked server.

Applicant again points out that the Office Action again did not specifically address claims 2, 7-12, 14, or 19.

III. Rejections under 35 USC §103(a)

Original claims 1-3, 5-15 and 17-22 stand rejected under 35 USC §103(a) as being unpatentable over McGarvey (6,643,774) in view of Kirby (5,898,784).

A prima facie case of obviousness is established when the Examiner provides one or more references that were available to the inventor and that teach a suggestion to combine or modify the references the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

Applicant respectfully believes the Examiner may have confused the difference between a cryptographic service and the cryptographic operations used to encrypt communications between the client and server. The cryptographic service that resides on the server performs cryptographic operations for the client. Thus, the client can off-load, for example, a computationally expensive cryptographic operation to a server that is optimized to perform that cryptographic operation.

The Examiner's references to McGarvey Fig. 6 and column 10, lines 33-36 do not teach such a service. The cited text simply teaches that communication between the server and client can be encrypted. Thus, when McGarvey's client delegates an operation to McGarvey's sever, McGarvey's server can access the same resources that the client can access and the McGarvey server and client can communicate using an encrypted data path.

With regards to McGarvey: McGarvey teaches techniques for allowing a server to use a client computer's (or user's) authority so that the server computer can access protected resources or perform protected services on behalf of the client (McGarvey column 2, lines 4-11; column 6, line 64 – column 7 line 16; and column 8, lines 52-56).

The problem addressed by McGarvey is how to allow a client computer to give a server the same access to protected data or services that the client has. It does this by delegating client authority to a server so that the server can access the protected data or services in place of the client. This delegation is accomplished by using a public key encryption system to establish trusted communication between a client, a server, and a private key system.

Nothing in McGarvey teaches to one skilled in the art a suggestion to modify McGarvey to include a networked server that provides cryptographic services (as that term is used in the application) to a client.

With regards to Kirby: Kirby teaches network tunneling and encryption techniques.

The problem addressed by Kirby is that of sending network packets through firewalls.

While Kirby recognizes the burden of encrypting and decrypting packets (Kirby: column 6, lines 25-40) Kirby suggests spreading the burden to multiple computers by terminating the virtual tunnels at the different computers.

Thus, nothing in Kirby teaches to one skilled in the art a suggestion to modify Kirby to include a networked server that provides cryptographic services to a client.

The Office Action asserts that McGarvey and Kirby would suggest a combination to one skilled in the art that would make the claimed invention obvious. However, the reason provided (that such a one would be "motivated to receive information at the server from the client utilizing the tunnel as taught in Kirby for determining the type of encryption algorithm used to encrypt the packet") indicates the Examiner's misunderstanding of the claimed invention. In the claimed invention, a client computer

requests a cryptographic service from a cryptographic server over the tunnel. The server then performs the requested cryptographic service. The requested service has nothing to do with the packets or the encryption algorithm of the packets sent over the tunnel.

Prior to the invention there were no cryptographic servers. Cryptographic operations were performed on the computer that needed the operation to be accomplished. Computationally expensive cryptographic operations thus were a significant load on these computers. By off-loading these cryptographic operations to a server that provides cryptographic services, the client can use its resources to perform other tasks while waiting for the results from the server.

Applicant respectfully traverses all assertions that cryptographic operations performed at the server to enable secure communication between the client and server read on the claimed invention. Cryptographic operations that are requested by the client of the server are those operations that could have been performed by the client.

Nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to a networked server that provides cryptographic services to a client.

Thus, previously presented **claim 1** is patentable. Previously presented **claim 13** and previously presented **claim 20** are a program product claim and a system claim (respectively) that are comparable with previously presented claim 1 and so are also patentable for the same reasons.

Original claims 2 and 14 depend on and further limit their respective independent claims that are patentable and thus claims 2 and 14 are also patentable.

Previously presented claims 3 and claim 15 depend on and further limit their respective parent claims that are patentable and thus claims 3 and 15 are also patentable.

Previously presented claim 21 depends on and further limits patentable claim 3 and thus claim 21 is also patentable.

Claims 4 and 16 have been canceled.

Previously presented claims 5 and 17 depend on and further limit their respective independent claims that are patentable and thus claims 5 and 17 are patentable. Furthermore, nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to off-load modular exponentiation from a client to a cryptographic server.

Previously presented claims 6 and 18 depend on and further limit their respective independent claims that are patentable. Thus claims 6 and 18 are also patentable.

Original claim 22 depends on and further limits patentable claim 21 and thus claim 22 is also patentable.

Previously presented claims 7-9 and 19; and original claims 10-12 depend on and further limit their respective parental claims that are patentable. Thus, claims 7-9, 10-12 and 19 are patentable.

The undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

PATENT

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,

DANIEL B. CURTIS
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com